

Note: The arresting officer is directed to serve the attached copy of the charge on the defendant at the time this warrant is executed.

Approved: Rosemary Nidiry  
ROSEMARY NIDIRY  
Assistant United States Attorney

Before: HONORABLE KEVIN NATHANIEL FOX  
United States Magistrate Judge  
Southern District of New York

12 MAG 1565

- - - - - x  
: UNITED STATES OF AMERICA : SEALED COMPLAINT  
: :  
- v. - : Violation of  
: 18 U.S.C. §§ 1349, 1029(b),  
: 1028A and 2  
ALI HASSAN, :  
a/k/a "Mr Badoo," :  
a/k/a "Mr.Badoo," :  
a/k/a "Badoo," : COUNTY OF OFFENSE:  
: NEW YORK  
: Defendant. :  
: :  
- - - - - x

SOUTHERN DISTRICT OF NEW YORK, ss.:

ALAN TRAN, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation (the "FBI"), and charges as follows:

COUNT ONE  
(Conspiracy to Commit Wire Fraud)

1. From on or about October 15, 2010, up to and including in or about July 2011, in the Southern District of New York and elsewhere, ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, and others known and unknown, willfully and knowingly, did combine, conspire, confederate and agree together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

2. It was a part and an object of the conspiracy that ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, and others known and unknown, willfully and knowingly having devised and intending to devise a scheme

and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds for the purpose of executing such scheme and artifice to defraud, in violation of Title 18, United States Code, Section 1343.

#### OVERT ACTS

3. In furtherance of the conspiracy, and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about November 5, 2010, ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, in Italy, posted an advertisement for the sale of stolen credit card numbers on a carding website which was hosted and could be accessed in the Southern District of New York.

b. Between on or about November 27, 2010 and on or about March 8, 2011, ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, in Italy, sent at least 12 e-mails to various co-conspirators not named herein containing information for at least 350 credit cards, including the account number, name and address of the account holder, expiration date, and the "card verification value" or "CVV" number.

(Title 18, United States Code, Section 1349.)

#### COUNT TWO

(Conspiracy to Commit Access Device Fraud)

4. From on or about October 15, 2010, up to and including in or about July 2011, in the Southern District of New York and elsewhere, ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit access device fraud, in violation of Title 18, United States Code, Section 1029.

5. It was a part and an object of the conspiracy that ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, and others known and unknown, would and

did knowingly and with intent to defraud, and affecting interstate and foreign commerce, possess fifteen and more devices which were counterfeit and unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(3).

#### Overt Acts

6. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about November 5, 2010, ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, in Italy, posted an advertisement for the sale of stolen credit card numbers on a carding website which was hosted and could be accessed in the Southern District of New York.

b. Between on or about November 27, 2010 and on or about March 8, 2011, ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, in Italy, sent at least 12 e-mails to various co-conspirators not named herein containing information for at least 350 credit cards, including the account number, name and address of the account holder, expiration date, and the "card verification value" or "CVV" number.

(Title 18, United States Code, Section 1029(b)(2).)

#### Count Three

(Aggravated Identity Theft)

7. From on or about October 15, 2010, up to and including in or about July 2011, in the Southern District of New York and elsewhere, ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, willfully and knowingly did transfer and possess, without lawful authority, a means of identification of another person, during and in relation to the felony violations charged in Counts One and Two of this Complaint, to wit, HASSAN transferred and possessed, among other things, names, addresses, and credit card account numbers of other persons in connection with his participation in a conspiracy to commit wire fraud as charged in Count One of this Complaint and his participation in a conspiracy to commit access device fraud as charged in Count Two of this Complaint.

(Title 18, United States Code, Sections 1028A(a) (1),  
1028A(b), and 2.)

The basis for my knowledge and for the foregoing charges are, in part and among other things, as follows:

8. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with other law enforcement agents, and my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

9. I have been a Special Agent with the FBI for approximately one year and seven months. For the past four months, I have been assigned to the computer intrusion squad in the FBI's New York Field Office. I have received training regarding computer technology, computer fraud, and white collar crimes.

#### BACKGROUND

10. Based on my training and experience, I have learned the following:

a. Carding: "Carding" refers to various criminal activities associated with stealing personal identification information and financial information belonging to other individuals - including the account information associated with credit cards, bank cards, debit cards, or other access devices - and using that information to obtain money, goods, or services without the victims' authorization or consent. For example, a criminal might gain unauthorized access to (or "hack") a database maintained on a computer server and steal credit card numbers and other personal information stored in that database. The criminal can then use the stolen information to, among other things: (1) buy goods or services online; (2) manufacture counterfeit credit cards by encoding them with the stolen account information; (3) manufacture false identification documents (which can be used in turn to facilitate fraudulent purchases); or (4) sell the stolen information to others who intend to use it for criminal purposes. "Carding" refers to the foregoing criminal activity

generally and encompasses a variety of federal offenses, including, but not limited to, identification document fraud, aggravated identity theft, access device fraud, computer hacking, wire fraud, and bank fraud.

b. Carding Forums: "Carding forums" are websites used by criminals engaged in carding ("carders") to facilitate their criminal activity. Carders use carding forums to, among other things: (1) exchange information related to carding, such as information concerning hacking methods or computer-security vulnerabilities that could be used to obtain personal identification information; and (2) buy and sell goods and services related to carding, for example, stolen credit card or debit card account numbers, hardware for creating counterfeit credit cards or debit cards, or goods bought with compromised credit card and debit card accounts. Carding forums often permit users to post public messages (postings that can be viewed by all users of the site), sometimes referred to as "threads." For example, a user who has stolen credit card numbers may post a public "thread" offering to sell the numbers. Carding forums also often permit users to communicate one-to-one through so-called "private messages." Because carding forums are, in essence, marketplaces for illegal activities, access is typically restricted to avoid law enforcement surveillance. Typically, a prospective user seeking to join a carding forum can only do so if other, already established users "vouch" for the prospective user, or if the prospective user pays a sum of money to the operators of the carding forum. User accounts are typically identified by a username and access is restricted by password. Users of carding forums typically identify themselves on such forums using aliases or online nicknames ("nics").

11. Based on my participation in the investigation of this matter, I know the following:

a. In or about June 2010, the FBI established an undercover carding forum (the "UC Site"), enabling users to discuss various topics related to carding and to communicate offers to buy, sell, and exchange goods and services related to carding, among other things.

b. The FBI established the UC Site as an online

meeting place where the FBI could locate cybercriminals, investigate and identify them, and disrupt their activities.<sup>1</sup> The UC Site was configured to allow the FBI to monitor and to record the discussion threads posted to the site, as well as private messages sent through the site between registered users. The UC Site also allowed the FBI to record the Internet protocol ("IP") addresses of users' computers when they accessed the site.<sup>2</sup>

c. Access to the UC Site was limited to registered members and required a username and password to gain entry. Various membership requirements were imposed from time to time to restrict site membership to individuals with established knowledge of carding techniques or interest in criminal activity. For example, at times new users were prevented from joining the site unless they were recommended by two existing users who had registered with the site, or unless they paid a registration fee.

d. New users registering with the UC Site were required to provide a valid e-mail address as part of the registration process. An e-mail message was sent to that email address containing registration instructions. In order to complete the registration process, the new user was required to open the e-mail, click on a link in it, and then enter an activation code specified in the e-mail message. The e-mail addresses entered by registered members of the site were collected by the FBI.

e. In the course of the undercover operation, the FBI contacted multiple affected institutions and/or individuals to advise them of discovered breaches in order to enable them to take appropriate responsive and protective measures. Based on information obtained through the site, the FBI estimates that it helped financial institutions prevent many millions of dollars in losses from credit card fraud and other criminal activity, and has alerted specific individuals regarding breaches of their personal email or other accounts.

---

<sup>1</sup> The registration process for the UC Site required users to agree to terms and conditions, including that their activities on the UC Site were subject to monitoring for any purpose.

<sup>2</sup> Every computer on the Internet is identified by a unique number called an Internet protocol ("IP") address, which is used to route information properly between computers.

f. At all times relevant to this Complaint, the server for the UC Site, through which all public and private messages on the UC Site were transmitted, was located in New York, New York.

### THE INVESTIGATION

12. As discussed in detail below, the investigation has revealed that ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, sold stolen credit card data. Specifically, HASSAN advertised on the UC Site offering to sell stolen credit card data; claimed to have obtained at least some of this stolen credit card information by hacking into a hotel booking website; and, over the course of approximately ten months, transmitted information from approximately 350 compromised credit card accounts over the Internet in e-mails to various co-conspirators.

#### The Defendant's Transmission of Stolen Credit Card Information to CW-1

13. Based on my involvement in monitoring the UC Site and my review of files and logs maintained by the FBI concerning the UC Site, I know that, on or about October 15, 2010, a new user registered on the UC Site with the username "Badoo." "Badoo" provided the e-mail address "elite.soft@hotmail.com" ("E-Mail Account-1") for the purpose of receiving registration instructions.<sup>3</sup>

14. From reviewing postings and private messages on the UC Site, I have learned that an individual using E-Mail Account-1 had a number of interactions, including those set forth below, with an individual who was acting at the FBI's direction as a site administrator on the UC Site ("CW-1").<sup>4</sup> The individual using E-Mail Account-1 communicated with CW-1 through

---

<sup>3</sup> On or about February 24, 2012, the Honorable Frank Maas, United States Magistrate Judge, authorized a search warrant of E-Mail Account-1.

<sup>4</sup> Based on my involvement in this investigation, I know that CW-1 was arrested by law enforcement and agreed to cooperate with the Government in the hope of receiving a reduced sentence. CW-1 has pleaded guilty to various charges pursuant to a cooperation agreement with the Government and is awaiting sentencing. CW-1's involvement in chats and private messages relating to the UC Site was done at the direction of, and with monitoring by, the FBI.



"MSN Messenger". ("MSN Messenger" is an instant-message system on the Internet allowing users to "chat" online, that is, to send text messages back-and-forth to one another in near real time. Users are identified by email addresses). I have reviewed private MSN Messenger "chats" of CW-1 which were electronically preserved. Based on my review of those chats, as well as my review of postings by "Badoo" on the UC Site and the contents of E-Mail Account-1, as detailed below, I believe that "Badoo," "Mr Badoo" (without a period and with a space), and "Mr.Badoo" (with a period and without a space), are the same individual: "Badoo" was the nickname he used to register on the UC Site and was the nickname that appeared in his postings on the UC Site; "Mr Badoo" was the nickname that appeared when he communicated through E-Mail Account-1; and "Badoo," "Mr.Badoo," or elite.soft@hotmail.com, the address for E-Mail Account-1, appeared when he communicated through MSN Messenger. Moreover, as discussed in further detail in ¶17 below, the investigation has revealed that this individual is ALI HASSAN, the defendant.

15. From my review of postings and private messages on the UC Site, I have learned the following:

a. On or about October 29, 2010, ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, using the nickname "Badoo," sent the following private message on the UC Site to CW-1: "can i bcome cc vendor? tell me what do i have to do."<sup>5</sup> CW-1 responded: "Sure thing, to become a vendor, you first must be a seller. You can reach me on icq or msn." From my participation in this investigation, I know that vendors on the UC Site had to submit their goods or services to administrators of the UC Site for review, in order to prove that the goods and/or services worked as advertised. The defendant was seeking CW-1's assistance in being designated a vendor on the UC Site. CW-1 responded that in order to be a vendor, the defendant would first need to be a seller, and asked the defendant to contact CW-1 via private messaging through either "MSN" or "ICQ" (another instant messaging system). CW-1 then explained: "[w]e will discuss what exactly you are claiming to sell, and see what type of demonstration you will provide for forum review to have you become a seller."

b. On or about November 1, 2010, the defendant, using E-Mail Account-1 and the on-line nickname "Mr.Badoo," told CW-1 in a chat over MSN Messenger that he had "CVVs" from

---

<sup>5</sup> Quotations from emails and online postings are reproduced substantially as they appear in the original text; that is, errors in spelling and punctuation have not been corrected.

"mostly all countries . . . I would like if u just review uk,usa , Canada and any other eueopean." Later in that same chat, "Mr.Badoo" stated, "it's the cc method, how do i take them . . .," and then explained that he obtained the credit card information through hotel booking information. Later on that same day, "Mr.Badoo" then sent CW-1 a file which "Mr.Badoo" claimed contained "faxes from [Website #1] to their hotel customer . . . i have about [Hotel #1] data . . . 2009, 2008 . . . 98% cc's are working i have other shops also :)." Based on my training and experience and involvement in this investigation, I believe that in these communications the defendant was explaining to CW-1, in connection with his request to be an approved vendor, that he had access to stolen credit card data from around the world, including the United States and Canada as well as the United Kingdom and other European countries, and the data he had from those credit cards included the "CVV" or "card verification value" number.<sup>6</sup> He then provided CW-1 with a sample of that credit card data so CW-1 - a site administrator - could verify it. In this chat, the defendant also explained that he obtained the credit card information for individuals registering at Hotel #1 through access to the records that Website #1, an on-line hotel registration website, provided to hotels.

c. On or about November 5, 2010, CW-1 chatted over MSN with the defendant, who was using the nickname "Badoo" and using E-Mail Account-1 as his MSN identifier. In this chat, the defendant gave CW-1 data from 20 U.S.-based credit cards and 25 non-U.S.-based credit cards to check. CW-1 then asked: "whats your replacement policy because from the 20 usa i received half do not work." The defendant responded: "i can replace my [Website #1] cc, in 24 hours." Based on my training and experience and involvement in this investigation, I believe that in this exchange, CW-1 had checked the card information provided by the defendant as part of the verification process described in ¶15a, and determined that many of the cards provided by the defendant were not valid credit cards. Later, in the same chat, CW-1 agreed to give the defendant seller status on the UC Site. Subsequently, in January 2011, the

---

<sup>6</sup> The "card verification value" or "cvv" number is a number, in addition to the credit card account number, that is found on credit cards and is designed to provide fraud prevention protection.

defendant sent CW-1 at least two more messages containing credit card information for an additional 34 cards.<sup>7</sup>

The Defendant's Transmission of Stolen Credit Card  
Information to Co-Conspirators

16. From reviewing postings and private messages on the UC Site, as well as the contents of E-Mail Account-1, I have learned that ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, using E-Mail Account-1 and the on-line nicknames "Badoo," "Mr Badoo," or "Mr.Badoo," had a number of interactions, including those set forth below, in which he transmitted stolen credit card information to various co-conspirators not named herein.

a. On or about November 2, 2010, a co-conspirator not named herein ("CC-1") posted the following on the UC Site: "I need a CC with high balance I have 7\$ LR some one plz pm me." Approximately 20 minutes later, ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, using the nickname "Badoo," responded on the same thread: "pm me, i got worldwide cc's also platinum + Gold thanks." Based on my training and experience and involvement in this investigation, I know that CC-1 was requesting a stolen credit card with a high balance, indicating that he would purchase it with funds in "LR" or "Liberty Reserve," an electronic form of currency, and asking to be contacted via "pm" or a private message. HASSAN responded that he had international credit cards, including platinum and gold cards.

b. On or about November 5, 2010, the defendant, using the nickname "Badoo," posted the following on the UC Site:

Hi, So here is my thread, 85% on Cp [Carderprofit.cc]<sup>8</sup>  
knows i am not reseller and selling my own Cc's So  
mostly buyers are really happy with my service, . . .  
. USA (visa,mc) 3\$ Each (Order in bulk will get 10%  
discount) USA (Amex) 5\$ Each (order in bulk will get  
10% discount) Canadian CC (MC,Visa,Amex,Disco) 7\$ Each  
(order in bulk 6\$ each) European Cc's 9\$ Each , German  
Cc's 15\$ Each . . . .

---

<sup>7</sup> The FBI has notified the relevant credit card companies regarding all the credit card information transmitted by the defendant discussed both in this paragraph and referenced throughout this Complaint.

<sup>8</sup> The name of the UC Site was "Carderprofit.cc".

Based on my training and experience and involvement in this investigation, I know that in the above post, the defendant provided a detailed explanation about his operation, including the types of credit cards he had to offer and the costs at which he was selling them. I have viewed the above post in the Southern District of New York as have other FBI agents involved in this investigation.

c. On or about November 7, 2010, a co-conspirator not named herein ("CC-2") sent the following private message on the UC Site to the defendant, who was using the nickname "Badoo": "hey yo im interested in buying cvv. whats ur msn/aim?" Based on my training and experience investigating carding schemes, I believe that in this exchange, CC-2 expressed an interest in buying stolen credit cards with CVVs from "Badoo" and asked for his contact information on instant messaging ("msn/aim"). Based on my review of records on the UC Site, I know that CC-2 registered as a user on the UC Site with the e-mail hellsatan@gmail.com. Four days after this communication, on or about November 11, 2010, an e-mail was sent from the defendant, using the nickname "Mr Badoo" and E-Mail Account-1, to the e-mail address hellsatan@live.ca, with an attachment containing information, including the account number, name and address of the account holder, expiration date, and the CVV number for 48 credit cards. The next day, on or about November 12, 2010, CC-2 sent the following private message on the UC Site to the defendant: "heyo i bought 50 cc from ya and got about 20 dead ones." Then, again, on November 13, 2010, CC-2 sent the following private message on the UC Site to the defendant: "hey my friend any chance you can get those cc by tonight or 2morrow early morning. . . ." Based on my training and experience, and involvement in this investigation, I believe that in these exchanges, CC-2 complained to the defendant that of the "50" (or approximately 50, as it was 48) credit cards the defendant had sold CC-2, about 20 did not work, and then asked when the defendant would send replacement credit cards.

d. E-mails from the defendant, using the nickname "Mr Badoo" and E-Mail Account-1, were sent again on or about November 16 and November 29, 2010 to the e-mail address hellsatan@live.ca, each with attachments, containing information, including the account number, name and address of the account holder, expiration date, and the CVV number for a combined total of 24 credit cards. These communications are consistent with the defendant sending CC-2 replacement credit card data as discussed in ¶16c above.

e. In total, in three e-mails, on or about November 11, November 16, and November 29, 2010, the defendant, using the nickname "Mr Badoo," provided hellsatan@live.ca information, including the account number, name and address of the account holder, expiration date, and the CVV number for 72 credit card accounts. Based on information from Visa and Mastercard, the FBI has confirmed that at least six Visa credit card numbers and at least seven Mastercard credit card numbers that the defendant passed in these e-mails corresponded to genuine accounts belonging to someone other than ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant. The FBI is awaiting confirmation for the remaining accounts.

f. On or about November 15, 2010, a co-conspirator not named herein ("CC-3") sent the following private message on the UC Site to the defendant, who was using the nickname "Badoo": "Can you send me a couple amex and one non-avs?" I know based on my training and experience that "amex" refers to American Express cards and "non-avs" refers to cards which do not support "AVS," an address verification service, and thus can be used without the address having to be verified. The defendant responded on or about November 15, 2010 with information, including the account number, name and address of the account holder, expiration date and the CVV number for four credit card accounts. From speaking with representatives of Visa and Mastercard, the FBI has confirmed that the credit card information transmitted in this e-mail was for one MasterCard and three Visa (not American Express) credit card accounts, and that each corresponded to a genuine account belonging to someone other than ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant.

g. On or about November 16, 2010, a co-conspirator not named herein ("CC-4") sent a private message on the UC Site to the defendant, who was using the nickname "Badoo": "Hi bro would you trade me some cvvs. I can offer you apple call ins or iphone serials. I cant pay money atm as i only have paypal. Thanks." The defendant responded: "pm me elite.soft@hotmail.com." I believe that CC-4 was asking the defendant if he could provide credit card account numbers along with their card verification values in exchange for serial numbers of various Apple products (which some carders used to try to fraudulently obtain free "replacement" products from Apple). The defendant then asked CC-4 to contact him via "pm" (or personal messaging) and provided the address of E-Mail Account-1.

h. On or about November 18, 2010, CC-3 again contacted the defendant, using the nickname "Badoo," via private message on the UC Site, saying the following: "I need you to send me some amex as soon as you get online please! . . . AMEX or Discover only!" The defendant responded on or about November 19, 2010 in a private message with information, including the account number, name and address of the account holder, expiration date of the card, and the CVV for six credit card accounts. Subsequently, on or about November 27, 2010, an e-mail was sent by the defendant, using the nickname "Mr Badoo" and E-Mail Account-1, to CC-3, with an attachment containing information, including the account number, name and address of the account holder, expiration date, and the CVV for nine additional credit card accounts. Based on information from Mastercard and Visa, the FBI has confirmed that of the card information sent by the defendant in this e-mail, at least one Visa card number and one MasterCard number corresponded to a genuine account belonging to someone other than ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant. (Based on the card information sent by the defendant it does not appear that he sent any AMEX or Discover cards, despite CC-3's specific request.) The FBI is awaiting confirmation for the remaining accounts.

i. On or about November 30, 2010, an e-mail was sent from the defendant, using the nickname "Mr Badoo" and E-Mail Account-1, to a co-conspirator not named herein ("CC-5") at a particular e-mail address (the "CC-5 E-Mail Address") with an attachment containing information, including the account number, name and address of the account holder, expiration date and the CVV numbers for 100 credit card accounts, including two with a name and address in Manhattan. I know based on my involvement in this investigation that an individual using the same nickname as CC-5 registered as a user on the UC Site with the CC-5 E-Mail Address, and that CC-5 offered to sell fake identification documents and passports, as well as stolen credit card account information, on the UC Site. From speaking with representatives of Visa and Mastercard, the FBI has confirmed that at least 14 Visa numbers and at least 18 MasterCard numbers that the defendant passed to CC-5 through E-Mail Account-1 corresponded to genuine accounts belonging to someone other than ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant. The FBI is awaiting confirmation for the remaining accounts.

### Identification of the Defendant

17. During the investigation, as noted above, the Government obtained a search warrant as well as registration records for E-Mail Account-1. From reviewing the registration records and the e-mails obtained pursuant to that search warrant, I have learned, in substance and among other things:

a. E-Mail Account-1 is registered in Italy. In addition, based on Internet Protocol (IP) address information, E-Mail Account-1 frequently accessed the Internet from Italy.

b. On or about October 25, 2010, ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, using the nickname "Badoo," sent a private message to a co-conspirator not named herein ("CC-6") on the UC Site with the subject line "i-pod to be shipped." The body of the private message gave the name "Ali Hassan" at an address in Milan, Italy (the "Milan Address"), and the message: "this is what you need, so i hope you will do it."

c. Certain documents containing personal identification information were found in E-Mail Account-1, further indicating that ALI HASSAN, the defendant, was the individual using E-Mail Account-1 and the on-line nicknames "Mr.Badoo," "Mr Badoo," and "Badoo." For example, between on or about February 15, 2012 and March 24, 2012, approximately 29 e-mail messages, each with a resume attached, were sent from E-Mail Account-1 to various addresses. All of the resumes were for an individual named "Ali Hassan" with the Milan Address - the same address "Badoo" provided for shipping the i-pod as discussed in ¶17b - listed as his home address. "Ali Hassan" with the Milan Address is the only individual for whom a resume was found in E-Mail Account-1.

d. A registration e-mail in E-Mail Account-1 from "E-Buy Gold" (EBG), an on-line gold currency website, listed the following in connection with E-Mail Account-1's registration:

You have changed your personal details on EBG website:  
Registered as: Individual  
Company Name: elite-soft  
First Name: ali  
Last Name: hassan  
Address: [Number and Street]  
City: faisalabad  
Zip Code: 38000

State/province: punjab  
Country: Pakistan  
E-mail: elite.soft@hotmail.com

e. An outgoing e-mail from E-Mail Account-1 dated March 17, 2011 contained as an attachment a document that appeared to be a letter addressed to the Government of Pakistan from an individual named "Ali Hassan." In the letter, the author stated that he was currently living in Italy and was seeking a visa to go to Australia, and requested that the Government of Pakistan provide him with a "police clearance certificate" that was required by the Australian Embassy; because he had sent his passport to the Australian Embassy to get the visa, he could not come to Pakistan himself.

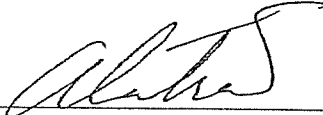
18. Accordingly, I believe that the individual described above as "Mr Badoo," "Mr.Badoo," and "Badoo," who advertised the sale of stolen credit cards on the UC Site and sent credit cards to various customers through E-Mail Account-1 and through the UC Site, is ALI HASSAN, the defendant.

19. From speaking with representatives of American Express, Visa, and MasterCard, I have confirmed that at least 62 credit card numbers the defendant passed to various individuals



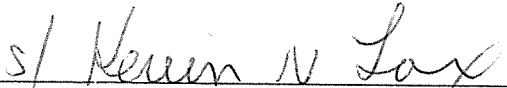
through E-Mail Account-1 and on the UC Site corresponded to genuine accounts belonging to individuals other than ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant.

WHEREFORE, I respectfully request that an arrest warrant be issued for ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.



ALAN TRAN  
Special Agent  
Federal Bureau of Investigation

Sworn to before me this  
12 day of June 2012



HON. KEVIN NATHANIEL FOX  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK